

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA**

BRITTANY VONBERGEN, *individually and
on behalf of all others similarly situated,*

Plaintiff,

v.

LIBERTY MUTUAL INSURANCE
COMPANY,

Defendant.

Case No. 2:22-cv-04880-GEKP

CLASS ACTION

JURY TRIAL DEMANDED

AMENDED CLASS ACTION COMPLAINT

Plaintiff Brittany Vonbergen brings this class action against Defendant Liberty Mutual Insurance Company and alleges as follows upon personal knowledge as to Plaintiff and Plaintiff's own acts and experiences, and, as to all other matters, upon information and belief, including investigation on conducted by Plaintiff's attorneys.

NATURE OF THE ACTION

1. "Since the advent of online behavioral advertising ('OBA') in the late 1990s, businesses have become increasingly adept at tracking users visiting their websites." *Popa v. Harriet Carter Gifts, Inc.*, 426 F. Supp. 3d 108, 111 (W.D. Pa. 2019) (citations omitted). This case involves one of the most egregious examples of such consumer tracking and Internet privacy violations.

2. Plaintiff brings this case as a class action under the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Cons. Stat. 5701, *et seq.* ("WESCA"). The case stems from Defendant's unlawful procurement of the interception of Plaintiff's and Class members'

electronic communications through the use of third party “session replay” spyware that allowed Defendant to watch and record Plaintiff’s and the Class members’ visits to its websites.

3. As discussed in detail below, Defendant procured and utilized “session replay” spyware from third party Session Replay Providers, namely Clicktale and Datadog, respectively, who contemporaneously intercepted Plaintiff’s and the Class members’ electronic computer-to-computer data communications with Defendant’s website, including how they interacted with the website, their mouse movements and clicks, keystrokes, search terms, information and PII inputted into the website, and pages and content viewed while visiting the website. Defendant facilitated a third party’s interception, recording, processing and storage of electronic communications created through the webpages visited by Plaintiff and the Class members, as well as everything Plaintiff and the Class members did on those pages, *e.g.*, what they searched for, what they looked at, the information and personal details that they inputted, and what they clicked on.

4. Defendant knowingly and intentionally procured undisclosed third parties to intercept the electronic communications at issue without the knowledge or prior consent of Plaintiff or the Class members. Defendant did so for its own financial gain and in violation of Plaintiff’s and the Class members’ rights to be free of intrusion upon their private affairs and to control information concerning their person under the WESCA.

5. The third party “session replay” spyware procured and utilized by Defendant is not a traditional website cookie, tag, web beacon, or analytics tool. It is a sophisticated computer software that allows the Session Replay Provider to contemporaneously intercept, capture, read, observe, re-route, forward, redirect, and receive incoming electronic communications to Defendant’s website. Plaintiff’s and the Class members’ electronic communications are then interpreted, reproduced, and stored at Defendant’s behest using outside vendor(s)’s services and

can later be viewed and utilized by Defendant as a session replay, which is essentially a video of a Class member's entire visit to Defendant's website, including all of their actions.

6. "Technological advances[.]" such as Defendant's use of session replay technology, "provide 'access to a category of information otherwise unknowable' and 'implicate privacy concerns' in a manner different from traditional intrusions as a 'ride on horseback' is different from 'a flight to the moon.'" *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1273 (9th Cir. 2019) (quoting *Riley v. California*, 573 U.S. 373, 393 (2014)).

7. The CEO of a major "session replay" software company – while discussing the merger of his company with another "session replay" provider – publicly exposed why companies like Defendant engage in recording visitors to their websites: "The combination of Clicktale and Contentsquare heralds an ***unprecedented goldmine of digital data*** that enables companies to interpret and predict the impact of any digital element -- including user experience, content, price, reviews and product -- on visitor behavior[.]" *See Contentsquare Acquires Clicktale to Create the Definite Global Leader in Experience Analytics*, available at www.prnewswire.com/news-releases/contentsquare-acquires-clicktale-to-create-the-definitive-global-leader-in-experience-analytics-300878232.html (last accessed May 10, 2021) (emphasis supplied). This CEO further admitted that "this unique data can be used to activate custom digital experiences in the moment via an ecosystem of over 50 martech partners. With a global community of customers and partners, ***we are accelerating the interpretation of human behavior online and shaping a future of addictive customer experiences.***" *Id.* (emphasis supplied).

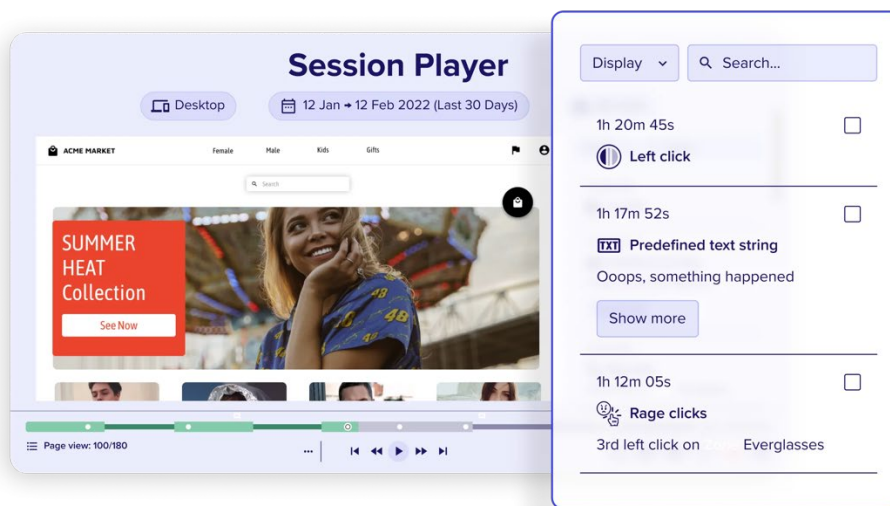
8. Unlike typical website analytics services that provide aggregate statistics, the third party session replay technology utilized by Defendant is intended to record and capture electronic communications on Defendant's website and then process those communications to create a

playback of individual browsing sessions, as if someone is looking over a Class members' shoulder when visiting Defendant's website. The technology also permits companies like Defendant to view the interactions of visitors on their website in real-time.

9. The following screenshot provides an example of a typical recording of a visit to a website captured utilizing session replay software, which includes mouse movements, keystrokes and clicks, search terms, content viewed, and personal information inputted by the website visitor:

DATA DOG:

The screenshot displays a browser session replay for a user named Albert Doe. The website shown is "COUCH CACHE", which has a navigation bar with links for CHAIRS, SOFAS, BEDDING, LIGHTING, MY PROFILE, and CART (0). The main content area is titled "Edit your profile" and contains a form with fields for Profile picture, Firstname (Doe), Lastname (John), and several masked input fields. The "Lastname" field is highlighted with a yellow dashed border. At the bottom of the form are "CANCEL" and "SAVE PROFILE" buttons. To the right of the main content is an "EVENT TIMELINE" panel showing a list of user actions and errors. The timeline includes events such as "Load Page /", "Load Page /department/lighting", "Click on IN STOCK on page /department/lighting", "Load Page /department/lighting/product/", "source error TypeError: Cannot read property 'addUserAction' of un...", "console error console error: TypeError: Cannot read property 'addUs...", "Load Page /cart", "Load Page /profile", "SPA Route Change /profile-edit", "Click on SAVE PROFILE on page /profile-edit", "source error TypeError: Converting circular structure to JSON --> s...", "console error console error: TypeError: Converting circular struct...", "source error ReferenceError: profile is not defined", "source error ReferenceError: profile is not defined", "console error console error: ReferenceError: profile is not defined", and "SPA Route Change /profile". The bottom of the screenshot shows a playback controls bar with a "Paused" button, a timeline slider, and a "Skip inactivity" toggle.

CLICKTALE:

10. The purported use of session replay technology is to monitor and discover broken website features. However, the extent and detail of the data collected by the Session Replay Providers for users of the technology, such as Defendant, far exceeds the stated purpose and Plaintiff's and the Class members' reasonable expectations when visiting websites like Defendant's. The technology not only allows the recording and viewing of a visitor's detailed electronic communications with a website, but also allows the user to create a detailed profile for each visitor to the site. Indeed, in an ongoing patent dispute, a well-known session replay provider openly admitted that this type of technology is utilized by companies like Defendant to make a profit: **"[the] software computes billions of touch and mouse movements and transforms this knowledge into profitable actions that increase engagement, reduce operational costs, and maximize conversion rates (i.e., the percentage of users who take desired actions on a website, such as purchasing a product offered for sale)."** *Content Square SAS v. Quantum Metric, Inc.*, Case No. 1:20-cv-00832-LPS, Compl. at ¶8, [DE 1] (D. Del. Jun. 22, 2020) (emphasis supplied).

11. Moreover, the collection and storage of page content may cause sensitive information and other personal information displayed on a page to leak to additional third parties. This may expose website visitors to identity theft, online scams, and other unwanted behavior.

12. In 2019, Apple warned application developers using session replay technology that they were required to disclose such tracking and recording to their users, or face being immediately removed from the Apple Store: “Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review Guidelines require that apps request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity.” <https://techcrunch.com/2019/02/07/apple-glassbox-apps/> (last visited November 15, 2021).

13. Consistent with Apple’s concerns, countless articles have been written about the privacy implications of recording user interactions during a visit to a website, including the following examples:

- (a) *The Dark Side of ‘Replay Sessions’ That Record Your Every Move Online*, located at <https://www.wired.com/story/the-dark-side-of-replay-sessions-that-record-your-every-move-online/> (last visited Nov. 14, 2022);
- (b) *Session-Replay Scripts Disrupt Online Privacy in a Big Way*, located at <https://www.techrepublic.com/article/session-replay-scripts-are-disrupting-online-privacy-in-a-big-way/> (last visited Nov. 14, 2022);
- (c) *Are Session Recording Tools a Risk to Internet Privacy?*, located at <https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/> (last visited Nov. 14, 2022);

- (d) *Session Replay is a Major Threat to Privacy on the Web*, located at <https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720> (last visited Nov. 14, 2022);
- (e) *Session Replay Scripts Could be Leaking Sensitive Data*, located at <https://medium.com/searchencrypt/session-replay-scripts-could-be-leaking-sensitive-data-5433364b2161> (last visited Nov. 14, 2022);
- (f) *Website Owners can Monitor Your Every Scroll and Click*, located at <https://www.digitalinformationworld.com/2020/02/top-brands-and-websites-can-monitor-your-every-scroll-and-click.html> (last visited Nov. 14, 2022); and
- (g) *Sites Using Session Replay Scripts Leak Sensitive User Data*, located at <https://www.helpnetsecurity.com/2017/11/20/session-replay-data-leak> (last visited Nov. 14, 2022).

14. In sum, Defendant procured the interception of the electronic communications of Plaintiff and the Class members through their visits to its website, causing them injuries, including violations of their substantive legal privacy rights under the WESCA, invasion of their privacy, intrusion upon their private affairs and potential exposure of their private information.

15. Through this action, Plaintiff seeks damages authorized by the WESCA on behalf of herself and the Class members, defined below, and any other available legal or equitable remedies to which they are entitled.

PARTIES

16. Plaintiff is, and at all times relevant hereto was, a natural person and a permanent resident of the State of Pennsylvania.

17. Defendant is, and at all times relevant hereto was, a corporation duly organized and validly existing under the laws of Massachusetts and maintains its principal place of business in Massachusetts. Defendant is therefore a citizen of Massachusetts.

JURISDICTION, VENUE AND STANDING

18. This Court has personal jurisdiction over Defendant under Pennsylvania's long arm statute. Pa. Const. Stat. § 5322. Defendant specifically directs, markets, and provides its business activities throughout the State of Pennsylvania, and makes its active commercial website, including Pennsylvania specific material, available to residents of Pennsylvania for those interested in entering into contracts over the Internet with Defendant. For example, Pennsylvania residents seeking to obtain an auto insurance quote from Defendant's website are specifically asked about their weekly commuting activities to New York and New Jersey. Indeed, Defendant's website contains marketing pages specific to Pennsylvania residents and allows residents of Pennsylvania to both submit information and make purchases utilizing the website. *See e.g., Pennsylvania Car Insurance*, <https://www.libertymutual.com/vehicle/auto-insurance/state/pennsylvania> (last accessed on January 18, 2023), *Pennsylvania home insurance*, <https://www.libertymutual.com/property/homeowners-insurance/state/pennsylvania> (last accessed on January 18, 2023). Plaintiff further is registered to do business in Pennsylvania under the fictitious name Liberty Mutual Insurance Agency and maintains at least 13 offices with insurance agents providing Defendant's services within the state of Pennsylvania. During the relevant time frame, Defendant solicited and processed Pennsylvania specific insurance quote forms submitted through its website and entered into contracts for the sale of services with residents of Pennsylvania that involved the knowing and repeated transmission of computer data over the Internet. This resulted in Defendant generating revenue from sales to residents of

Pennsylvania, as well accepting payments from Pennsylvania residents through the site and ultimately providing services to Pennsylvania residents that originated through the site. Therefore, Defendant has purposefully availed itself of the privileges of conducting activities within the State of Pennsylvania. Plaintiff's and the Class members' claims arise directly from Defendant's operation of its website and its targeting of Pennsylvania.

19. Further, this Court has personal jurisdiction over Defendant because Defendant's tortious conduct against Plaintiff occurred in substantial part within this District and because Defendant committed the same wrongful acts to other individuals within this judicial District, such that Defendant's acts complained of herein occurred within this District, subjecting Defendant to jurisdiction here. *See Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 132 (3d Cir. 2022) ("the place of interception is the point at which the signals were routed to [the session replay provider's] servers"). Thus, Defendant knew or should have known that it was causing harm to those individuals while they were in Pennsylvania such that it was foreseeable to Defendant that its interceptions would harm Plaintiff and other similarly-situated individuals located in Pennsylvania.

20. This court has subject matter jurisdiction under 28 U.S.C. § 1332(d)(2) because at least one member of the putative class, including Plaintiff, is a citizen of Pennsylvania, and Defendant is a citizen of Massachusetts, thus CAFA's minimal diversity requirement is met. Additionally, Plaintiff seeks, at minimum, \$1,000.00 in damages for each violation, which, when aggregated among a proposed class of over 5,000, exceeds the \$5,000,000 threshold for federal court jurisdiction under the Class Action Fairness Act ("CAFA").

21. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b) and (c) because Defendant is deemed to reside in any judicial district in which it is subject to personal jurisdiction,

and because a substantial part of the events or omissions giving rise to the claim occurred in this District, and because Plaintiff was injured in this District.

22. Plaintiff has Article III standing to maintain this action because she suffered a cognizable and particularized injury as a result of Defendant's violations of the WESCA, and because she is not requesting an advisory opinion from this Court. Thus, Plaintiff has a sufficient stake in a justiciable controversy and seeks to obtain judicial resolution of that controversy. At common law, Defendant's conduct would amount to an invasion of privacy, such as intrusion upon seclusion, of which the intrusion itself is sufficient injury for standing. *See Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1111 (9th Cir. 2020) ("under the privacy torts that form the backdrop for these modern [wiretapping] statutes, the intrusion itself makes the defendant subject to liability... Thus, historical practice provides [] support... for the conclusion that a wiretapping plaintiff need not allege any further harm to have standing"); *see also Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 423, (2013) (the "interception of a private [communication] amounts to an injury that is 'concrete and particularized'.").

FACTS

23. Defendant owns and operates the following website: libertymutual.com.
24. Plaintiff most recently visited Defendant's website on or about March of 2022.
25. During this visit, Plaintiff filled out an online auto insurance quote form specific to Pennsylvania.
26. While filling out this form, Plaintiff was required to communicate her personal information including, but not limited to:

- 1) her zip code; 2) name; 3) birthdate; 4) address; 5) how long she had lived at that address; 6) her email; 7) her license plate number or Vehicle Identification Number; 8) whether she owned, financed, or leased her vehicle; 9) her frequency of commuting to New York or New Jersey; 10)

where she kept her vehicle; 11) the year she bought her vehicle; 12) whether she was married or in a civil union; 13) her gender identity; 14) how old she was when she got her license; 15) her phone number; 16) whether she had current auto insurance and when she began that insurance; 17) details about that prior insurance coverage; 18) her employment status; 19) her highest level of education completed; and 20) whether she owned or rented her home.

27. Plaintiff was in Pennsylvania during her visit to Defendant's website.

28. During her visit to the website and completion of the online form, Plaintiff, through her computer and/or mobile device, transmitted substantive information via electronic communications in the form of instructions to Defendant's computer servers utilized to operate the website.¹ The commands were sent as messages instructing Defendant what content was being viewed, clicked on, requested and/or inputted by Plaintiff. By way of example, when filling out her online insurance quote form, Plaintiff was asked whether she owned or rented her home. Plaintiff clicked the selection for "rent". This interaction caused an electronic communication to be sent conveying that Plaintiff had selected that option and substantively expressed the message that she rented her home, which triggered the online form to proceed to the next question. This process applied with the same force for all of the personal information communicated by Plaintiff through her interactions with the online quote form, whether by clicking a selection (like home rental, gender identity, or highest level of education) or by inputting information via keystrokes (like license plate number, when she bought her vehicle, when she purchased her previous insurance).

¹ These communications occur through the Hypertext Transfer Protocol ("HTTP"). HTTP works as a request-response protocol between a user and a server as the user navigates a website. A GET request is used to request data from a specified source. A POST request is used to send data to a server. *See HTTP Request Methods*, located at https://www.w3schools.com/tags/ref_httpmethods.asp (last visited November 16, 2022).

29. The communications sent by Plaintiff to Defendant's (and unknowingly to the Session Replay Provider(s)'s) servers included, but were not limited to, the following actions taken by Plaintiff while on the website: mouse clicks and movements, keystrokes, search terms, information and PII inputted and communicated by Plaintiff, pages and content viewed by Plaintiff, scroll movements, and copy and paste actions.

30. Defendant responded to Plaintiff's electronic communications by processing and supplying – through its website – the information inputted and requested by Plaintiff. *See Revitch v. New Moosejaw, LLC*, No. 18-cv-06827-VC, 2019 U.S. Dist. LEXIS 186955, at *3 (N.D. Cal. Oct. 23, 2019) (“This series of requests and responses — whether online or over the phone — is communication.”); *see also Popa v. Harriet Carter Gifts, Inc.*, No. 21-2203, 2022 U.S. App. LEXIS 28799 (3d Cir. Oct. 18, 2022).

31. At almost exactly the same moment that Plaintiff sent communications to Defendant's servers, the session replay software procured by Defendant instantaneously created a duplicate request-and-response communication for each of Plaintiff's actions and routed these communications to the Session Replay Provider's servers.

32. Plaintiff reasonably expected that her visit to Defendant's website would be private and that Defendant would not have procured a third party that was tracking, recording, and/or watching Plaintiff as she browsed, interacted with the website, and filled out the personal details she communicated through the online insurance quote form, particularly because Plaintiff was not presented with any type of pop-up disclosure or consent form alerting Plaintiff that her visit to the website was being recorded by Defendant through a third party.

33. Plaintiff reasonably believed that she was interacting privately with Defendant's website, and not that she was being recorded and that those recordings would be captured and

transmitted by and to third party servers that Plaintiff was unaware of, where they would be processed by that third party and could later be watched by Defendant's employees, or worse yet, live while Plaintiff was on the website.

34. Upon information and belief, over at least the past two years, Defendant has had embedded within its websites' code and has continuously operated at least one, and for some period two independent, session replay software script² that were provided by a third party (a "Session Replay Provider"). The session replay spyware was always active and intercepted every incoming data communication to Defendant's website the moment a visitor accessed the site.

35. The Session Replay Provider(s) that provided the session replay spyware to Defendant are not a provider of wire or electronic communication services, or an internet service provider.

36. Defendant is not a provider of wire or electronic communication services, or an internet service provider.

37. Defendant's use of session replay spyware was not instrumental or necessary to the operation or function of Defendant's websites or business.

38. Defendant's use of session replay spyware through Session Replay Providers to intercept Plaintiff's electronic communications was not instrumental or necessary to Defendant's provision of any of its goods or services. Rather, the level and detail of information surreptitiously collected by Defendant's Session Replay Provider(s) indicates that the only purpose was to gain an unlawful understanding of the habits and preferences of users to its website for Defendant's own benefit.

² A script is a sequence of computer software instructions.

39. Defendant's use of session replay spyware to intercept Plaintiff's electronic communications did not facilitate, was not instrumental, and was not incidental to the transmission of Plaintiff's or the Class members' electronic communications with Defendant's website.

40. Upon information and belief, during Plaintiff's visit to Defendant's website, Defendant utilized session replay spyware procured from third parties to intentionally and contemporaneously intercept the substance of Plaintiff's electronic communications with Defendant's website, including mouse clicks and movements, keystrokes, search terms, information and PII inputted by Plaintiff, pages and content viewed by Plaintiff, and scroll movements, and copy and paste actions. In other words, Defendant utilized its Session Replay Provider(s) to intercept, record, process and store electronic communications conveying everything Plaintiff did on the webpages visited by Plaintiff i.e. what Plaintiff searched for, what Plaintiff looked at, and the detailed personal information that Plaintiff inputted.

41. The session replay spyware intentionally utilized by Defendant contemporaneously intercepted the electronic computer-to-computer data communications between Plaintiff's computer and/or mobile device and the computer servers and hardware utilized by Defendant to operate its website – as the communications were transmitted from Plaintiff's computer and/or mobile device to Defendant's computer servers and hardware – and copied and sent and/or re-routed the communications to a storage file within the Session Replay Provider(s)'s server(s). The intercepted data was transmitted contemporaneously to the Session Replay Provider(s) server(s) as it was sent from Plaintiff's computer and/or mobile device.

42. The relevant facts regarding the full parameters of the communications intercepted and how the interception occurred are solely within the possession and control of Defendant.

43. The session replay spyware utilized by Defendant is not a website cookie, standard analytics tool, tag, web beacon, or other similar technology.

44. Unlike the harmless collection of an internet protocol address, the data collected by Defendant identified specific information inputted and content viewed (ex. Plaintiff's gender identity), and thus revealed personalized and sensitive information about Plaintiff including her internet activity and habits.

45. The electronic communications intentionally intercepted at Defendant's behest were content generated through Plaintiff's intended use, interaction, and communication with Defendant's website relating to the substance, purport, and/or meaning of Plaintiff's communications with the website, *i.e.*, mouse clicks and movements, keystrokes, search terms, information and PII inputted by Plaintiff, and pages and content clicked on and viewed by Plaintiff. Moreover, the electronic communications stemming from Plaintiff's interactions with the online insurance quote form included conveying highly personal content as described above.

46. The electronic communications intentionally intercepted by Defendant were not generated automatically and were not incidental to Plaintiff's communications.

47. The session replay spyware utilized by Defendant intercepted, copied, replicated, and sent the data to the Session Replay Provider(s) in a manner that was undetectable by Plaintiff.

48. Plaintiff's electronic data communications were then, processed, interpreted, stored and reproduced by Defendant and/or the Session Replay Provider(s).

49. The electronic data communications were not only intercepted and stored, but could also be used by Defendant to create a video playback of Plaintiff's visit to the website, displaying the content communicated by Plaintiff during her interactions with the site. Additionally, upon

information and belief, the session replay technology procured by Defendant gave Defendant the ability to view Plaintiff's website visits live in real-time as they were occurring.

50. Defendant's procured interception of Plaintiff's electronic communications allowed Defendant to capture, observe, and divulge Plaintiff's personal details, interests, browsing history, queries, and habits as she interacted with and browsed Defendant's website.

51. Upon information and belief, Defendant similarly procured the interception of the electronic communications of at least 5,000 individuals located in Pennsylvania who visited Defendant's website.

52. Defendant utilized third party spyware embedded within its website to intercept the communications at issue.

53. Defendant never alerted or asked Plaintiff or the Class Members for permission to have its Session Replay Provider(s) intercept and record their visits to Defendant's website using "session replay" spyware.

54. Plaintiff and the Class members never consented to interception of their electronic communications by Defendant and/or its Session Replay Provider(s) or anyone acting on Defendant's behalf, and they were never given the option to opt out of Defendant's recording.

55. At no point in time did Plaintiff or the Class members provide Defendant, its employees, or agents with consent to intercept their electronic communications using "session replay" spyware.

56. At no point in time did Plaintiff or the Class members specifically, clearly, and unmistakably consent to Defendant's use of a third party to intercept and record their electronic communications using "session replay" spyware.

57. At no point in time did Plaintiff or the Class members specifically, clearly, and unmistakably consent to Defendant's use of a third party to intercept and record their visits to Defendant's website using "session replay" spyware.

58. At no point in time did Plaintiff or the Class members impliedly consent to Defendant's use of a third party to intercept and record their electronic communications, as no reasonable person could assume that by communicating with Defendant's website, the substance of those electronic communications would be intercepted, captured, read, observed, re-routed, forwarded, interpreted, reproduced, and stored by an undisclosed third party Session Replay Provider.

59. Plaintiff and the Class members did not have a reasonable opportunity to discover Defendant's unlawful interceptions because Defendant did not disclose the third party interception nor seek consent from Plaintiff and the Class members prior to interception of their communications.

60. Plaintiff and the Class members never clicked or otherwise agreed to any disclosure or consent form authorizing Defendant to use a third party Session Replay Provider to intercept Plaintiff's and the Class members' electronic communications using "session replay" spyware.

61. Defendant's third party session replay spyware intercepted Plaintiff's and the Class members' electronic communications from the moment they landed on Defendant's website, and before they had an opportunity to even consider consenting or agreeing to any privacy or terms of use policy on the website. In other words, Defendant's unlawful interception occurred before Plaintiff and the Class members were given an opportunity to review, let alone consent, to any language that Defendant may claim purportedly authorized its violations of the WESCA. *See*

Javier v. Assurance IQ, LLC, No. 21-16351, 2022 U.S. App. LEXIS 14951, at *5 (9th Cir. May 31, 2022).

62. In fact, Defendant's website's privacy policy does not appear when completing an online Auto Insurance quote until "Step 3", multiple pages after Plaintiff and the Class members' had inputted personal information that was being intercepted and recorded. Moreover, the hyperlink is seemingly only displayed relating to the use of "automatically dialed calls" to a consumer's phone number and includes the language "Your consent isn't required to purchase a policy." On other online quote forms, such as Defendant's Renters Insurance form, the privacy policy does not appear as a hyperlink at all.

63. Moreover, Defendant's website failed to explicitly alert or otherwise notify Plaintiff and the Class members that Defendant would be utilizing session replay spyware to facilitate an undisclosed third party's monitoring and recording of their interactions with Defendant's website.

64. Additionally, upon immediately landing on Defendant's website, Plaintiff and the Class members were not alerted that by entering the website Defendant would unilaterally attempt to bind them to Defendant's terms of use or privacy policy. Indeed, the landing page to Defendant's website not only fails to advise visitors that Defendant is using a third party to intercept their electronic communications, it does not contain any type of conspicuous disclosure regarding Defendant's terms of use or privacy policy.

65. Plaintiff and the Class members were not immediately required to click on any box or hyperlink containing Defendant's terms of use or privacy policy upon visiting the website or in order to navigate through the website.

66. Plaintiff and the Class members were not placed on notice of Defendant's terms and policies or privacy policy upon immediately visiting the website. Instead, Defendant's terms of use and privacy policy are buried at the bottom of Defendant's website homepage where Plaintiff and the Class members were unable to see them. These inconspicuous footer hyperlinks were not present on the various pages of Defendant's quote forms. Plaintiff and the Class members were thus not on inquiry notice of Defendant's terms of use and privacy policy. *See Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1177 (9th Cir. 2014).

67. Defendant does not require visitors to its website to immediately and directly acknowledge that the visitor has read Defendant's terms of use or privacy policy before proceeding to the site or beginning to complete an online insurance quote form. In other words, Defendant's website does not immediately direct visitors to the sites to the terms of use or privacy policy, and do not require visitors to click on a box to acknowledge that they have reviewed the terms and conditions/policy in order to proceed to the website.

68. Upon information and belief, at least one of the purposes of Defendant's procured interception of Plaintiff's and the Class members' electronic communications was to allow Defendant to learn of Plaintiff's and the Class members' personal details, preferences and likes, which would then be used to market Defendant's services and goods to Plaintiff and the Class members.

69. The surreptitious third party interception of Plaintiff's and the Class members' electronic communications procured by Defendant caused Plaintiff and the Class members harm, including violations of their substantive legal privacy rights under the WESCA, invasion of privacy, intrusion upon seclusion, invasion of their rights to control information concerning their person, and/or the exposure of their private information. Indeed, at common law, the intrusion into

Plaintiff's and the Class members' private lives is of itself a cognizable injury. Moreover, Defendant's practices caused harm and a material risk of harm to Plaintiff's and the Class Members' privacy and interest in controlling their personal information, habits, and preferences.

CLASS ALLEGATIONS

PROPOSED CLASS

70. Plaintiff brings this lawsuit as a class action on behalf of all other similarly situated persons pursuant to Federal Rule of Civil Procedure 23. The "Class" that Plaintiff seeks to represent is defined as:

All persons residing within the State of Pennsylvania (1) who visited Defendant's website and (2) whose electronic communications were intercepted by Defendant or on Defendant's behalf (3) without their prior consent.

71. Defendant and its employees or agents are excluded from the Class. Plaintiff reserves the right to modify or amend the Class definitions, as appropriate, during the course of this litigation.

NUMEROSITY

72. The Class members are so numerous that individual joinder of all Class members is impracticable. Upon information and belief, Defendant intercepted the electronic communications of over 5,000 individuals. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include notice on Defendant's website, U.S. Mail, electronic mail, Internet postings, and/or published notice.

73. The identities of the Class members are unknown at this time and can be ascertained only through discovery. Identification of the Class members is a matter capable of ministerial determination from Defendant's records kept in connection with its unlawful interceptions.

COMMON QUESTIONS OF LAW AND FACT

74. There are numerous questions of law and fact common to the Class which predominate over any questions affecting only individual members of the Class. Among the questions of law and fact common to the Class are:

- (1) Whether Defendant violated the WESCA;
- (2) Whether Defendant intercepted or procured another to intercept Plaintiff's and the Class members' electronic communications;
- (3) Whether Defendant disclosed to Plaintiff and the Class Members that it was intercepting their electronic communications;
- (4) Whether Defendant secured prior consent before intercepting Plaintiff's and the Class members' electronic communications; and
- (5) Whether Defendant is liable for damages, and the amount of such damages.

75. The common questions in this case are capable of having common answers. If Plaintiff's claim that Defendants routinely intercepts electronic communications without securing prior consent is accurate, Plaintiff and the Class members will have identical claims capable of being efficiently adjudicated and administered in this case.

TYPICALITY

76. Plaintiff's claims are typical of the claims of the Class members, as they are all based on the same factual and legal theories.

PROTECTING THE INTERESTS OF THE CLASS MEMBERS

77. Plaintiff is a representative who will fully and adequately assert and protect the interests of the Class and has retained competent counsel. Accordingly, Plaintiff is an adequate representative and will fairly and adequately protect the interests of the Class.

SUPERIORITY

78. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the claims of all members of the Class is economically unfeasible and procedurally impracticable. While the aggregate damages sustained by the Class are potentially in the millions of dollars, the individual damages incurred by each member of the Class resulting from Defendant's wrongful conduct are too small to warrant the expense of individual lawsuits. The likelihood of individual Class members prosecuting their own separate claims is remote, and, even if every member of the Class could afford individual litigation, the court system would be unduly burdened by individual litigation of such cases.

79. The prosecution of separate actions by members of the Class would create a risk of establishing inconsistent rulings and/or incompatible standards of conduct for Defendant. For example, one court might enjoin Defendant from performing the challenged acts, whereas another may not. Additionally, individual actions may be dispositive of the interests of the Class, although certain class members are not parties to such actions.

COUNT I**Violations of the WESCA, 18 Pa. Cons. Stat. 5701, *et seq.*
(On Behalf of Plaintiff and the Class)**

80. Plaintiff re-alleges and incorporates the foregoing allegations as if fully set forth herein.

81. The Pennsylvania Wiretap and Electronic Surveillance Control Act (the "Act") prohibits (1) the interception or procurement of another to intercept any wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication; and (3) the intentional use of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was

obtained through the interception of a wire, electronic, or oral communication. 18 Pa. Cons. Stat. § 5703.

82. An “intercept[ion]” is the “[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device”. *See* 18 Pa. Cons. Stat. § 5702.

83. Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use, a wire, electronic, or oral communication in violation of the Act is subject to a civil action for (1) actual damages, not less than liquidated damages computed at the rate of \$100/day for each violation or \$1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys’ fees and other litigation costs incurred. 18 Pa. Cons. Stat. § 5725(a).

84. Defendant procured at least one, and at some time two independent, third party Session Replay Providers to automatically and secretly spy on, and intercept, Defendant’s website visitor’s electronic communications with Defendant in real-time.

85. To facilitate this wiretap, Defendant procured and installed its Session Replay Provider(s)’s software code on its website.

86. The session replay software code procured from the Session Replay Provider(s) by Defendant is a sophisticated system capable of capturing, recording, interpreting, reformatting, and processing electronic communications, and is therefore an “electronic, mechanical, or other device” as defined by the WESCA. *See* 18 Pa. Cons. Stat. § 5702.

87. The session replayed software code procured from the Session Replay Provider(s) by Defendant is not a “tracking device” because, as stated above, it is a sophisticated system with capabilities well beyond “*only* the tracking of the movement of a person or object.” *See* 18 Pa. Cons. Stat. § 5702.

88. Upon information and belief, Defendant knew that its Session Replay Provider(s) would add the contents of its visitor's private electronic communications, including but not limited to the personal information they communicated in their insurance quote forms, procured through the wiretap, to its back-end database, resulting in the unauthorized disclosure of such information to the Session Replay Provider(s) and risking the further disclosure of that information to others.

89. Defendant intentionally procured the interception of the content of Defendant's website visitors' private electronic communications in real-time, including the detailed personal information they communicated through the online quote form.

90. Plaintiff and the putative class members engaged in electronic communications with Defendant through use of Defendant's website, as their interactions with the website transferred "signs, signals, writing, images, sounds, data or intelligence" and their interactions were not wire or oral communications, a communication made through a tone-only paging device, or communications from a tracking device. *See* 18 Pa. Cons. Stat. § 5702

91. Plaintiff and the putative class members had a justified and reasonable expectation under the circumstances that their private electronic communications, including the contents of their personal details as described above, would not be intercepted by and exposed to an undisclosed third party. *See In re Google Inc.*, 806 F.3d 125, 151 (3d Cir. 2015); *see also In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 293-94 (3d Cir. 2016).

92. Nonetheless, Defendant employed its Session Replay Provider(s) to intercept the content of Plaintiff's and the putative class members' electronic communications with Defendant.

93. Because the code is secret and encrypted, Plaintiff and the putative class members were not aware that their electronic communications were being intercepted by Defendant's Session Replay Provider(s).

94. Plaintiff and the putative class members did not give prior consent to having their communications intercepted by Defendant or its Session Replay Provider(s).

95. By procuring its Session Replay Provider(s) to intercept, record, interpret, reproduce and store Plaintiff's and the Class members private electronic communications for its own purposes without prior consent, Defendant violated 18 Pa. Cons. Stat. § 5703(1), (2) and (3).

96. At all times pertinent hereto, Defendant's conduct was knowing and intentional.

97. As a result of Defendant's conduct, and pursuant to § 5725 of the WESCA, Plaintiff and the other members of the putative Class were harmed and are each entitled to actual damages, liquidated damages, punitive damages, reasonable attorneys' fees and costs. 18 Pa. Cons. Stat § 5725(a).

WHEREFORE, Plaintiff, on behalf of herself and the other members of the Class, prays for the following relief:

a. An order certifying the Class and appointing Plaintiff as Class Representative and her counsel as Class Counsel;

b. An award of actual damages, statutory damages, liquidated damages, and/or punitive statutory damages;

c. An award of reasonable attorney's fees and costs; and

d. Such further and other relief the Court deems reasonable and just.

JURY DEMAND

Plaintiff and Class Members hereby demand a trial by jury on all issues so triable.

DOCUMENT PRESERVATION DEMAND

Plaintiff demands that Defendant take affirmative steps to preserve all records, lists, electronic databases or other itemizations associated with the allegations herein, including all

records, lists, electronic databases or other itemizations in the possession of any vendors, individuals, and/or companies contracted, hired, or directed by Defendant to assist in sending the alleged communications.

Dated: January 31, 2023

Respectfully Submitted,

By: **MARCUS ZELMAN LLC**

/s/ Ari H. Marcus
Ari H. Marcus, Esq. (Pennsylvania Bar
No. 322283)
701 Cookman Avenue, Suite 300
Asbury Park, New Jersey 07712
Telephone: (732) 695-3282
Facsimile: (732) 298-6256
Ari@marcuszelman.com
Counsel for Plaintiff and Proposed Class

CERTIFICATION PURSUANT TO LOCAL RULE 11.2

I, Ari H. Marcus, the undersigned attorney of record for Plaintiff, do hereby certify to my own knowledge and based upon information available to me at my office, the matter in controversy is not the subject of any other action now pending in any court or in any arbitration or administrative proceeding.

Dated: January 31, 2023

/s/ Ari H. Marcus
Ari H. Marcus, Esq.